Managing The Insider Threat: What Every Organization Should Know

8.8.13 • 9:00 AM ET-5:00 PM ET

Illicit Cyber Activity Involving Fraud by Randy Trzeciak

Randy Trzeciak
Technical Manager - CERT Enterprise Threat and Vulnerability Management Team &
CERT Insider Threat Center

Randy is Technical Manager of CERT's Enterprise Threat and Vulnerability Management Team and the CERT Insider Threat Center at Carnegie Mellon University's Software Engineering Institute. The team's mission is to assist organizations in improving their security posture and incident response capability by researching technical threat areas, developing and conducting information security assessments, and providing information, solutions and training for preventing, detecting, and responding to illicit activity.

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **08 AUG 2013**	2. REPORT TYPE	3. DATES COVERED **00-00-2013 to 00-00-2013**

4. TITLE AND SUBTITLE **Illicit Cyber Activity Involving Fraud by Randy Trzeciak**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Carnegie Mellon University,Software Engineering Institute,Pittsburgh,PA,15213**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**27**	

This Research Study

Technical and behavioral patterns were extracted from 80 fraud cases—67 insider and 13 external—that occurred between 2005 and the present.

These cases were used to develop insights and risk indicators to help private industry, government, and law enforcement more effectively prevent, deter, detect, investigate, and manage malicious insider activity within the banking and finance sector.

This study was

- funded by the U.S. Department of Homeland Security's Science and Technology Directorate
- completed by the CERT® Insider Threat Center collaborating with the U.S. Secret Service

What Is Insider Fraud?

Malicious Insider - a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems [1]

Insider Fraud - a malicious insider's use of IT for the unauthorized modification, addition, or deletion of an organization's data (not programs or systems) for personal gain or the theft of information leading to an identity crime [2]

Identity Crime - the misuse of personal or financial identifiers in order to gain something of value and/or facilitate some other criminal activity

[1] Cappelli, D. M.; Moore, A. P.; Trzeciak, R. F.; & Shimeall, T. J. *Common Sense Guide to Prevention and Detection of Insider Threat, 3rd Edition—Version 3.1*. Software Engineering Institute, Carnegie Mellon University and CyLab. http://www.cert.org/archive/pdf/CSG-V3.pdf (2009).

[2] Weiland, Robert M.; Moore, Andrew P.; Cappelli, Dawn M.; Trzeciak, Randall F.; & Spooner, Derrick. *Spotlight On: Insider Threat from Trusted Business Partners*. Software Engineering Institute and CyLab, Carnegie Mellon University, 2010. http://www.cert.org/archive/pdf/TrustedBusinessPartners0210.pdf

Research Findings

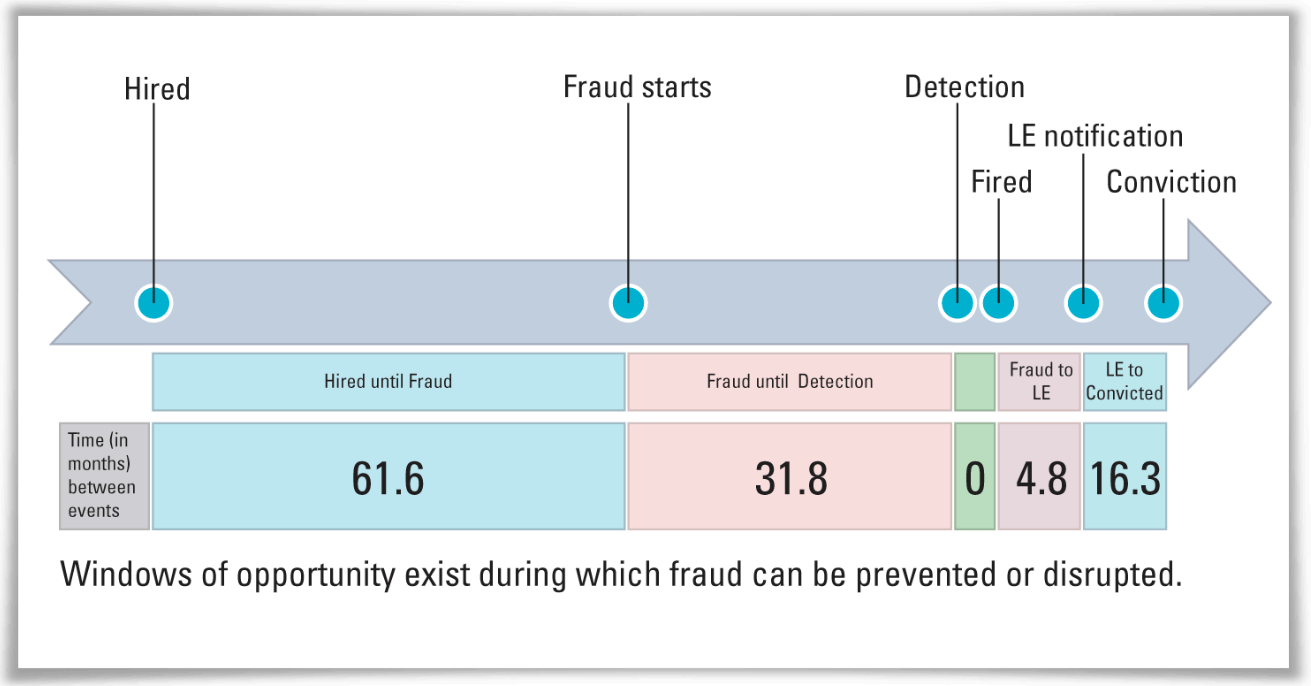
Our case analyses yielded six findings based on trends and descriptive statistics observed in the case files.

The majority of the 80 organizations impacted by these crimes are included in the banking and finance industry.

This industry includes retail, commercial, and investment banks; accounting firms; credit card issuers; federal credit unions; insurance providers; while some are financial departments of retail businesses (automobile, builders, employee benefit providers, employee staffing, engineering, fashion, home improvement, transportation) and federal, state, and local governments.

Finding One: Low and Slow

Criminals who executed a "low and slow" approach accomplished more damage and escaped detection for longer.



	Hired until Fraud	Fraud until Detection		Fraud to LE	LE to Convicted
Time (in months) between events	61.6	31.8	0	4.8	16.3

Windows of opportunity exist during which fraud can be prevented or disrupted.

There are, on average, over 5 years between a subject's hiring and the start of the fraud. There are 32 months between the beginning of the fraud and its detection.

Finding One: A Case Example

Subject: An accountant at a CPA firm with good performance who had sole responsibility for accounts of two client companies

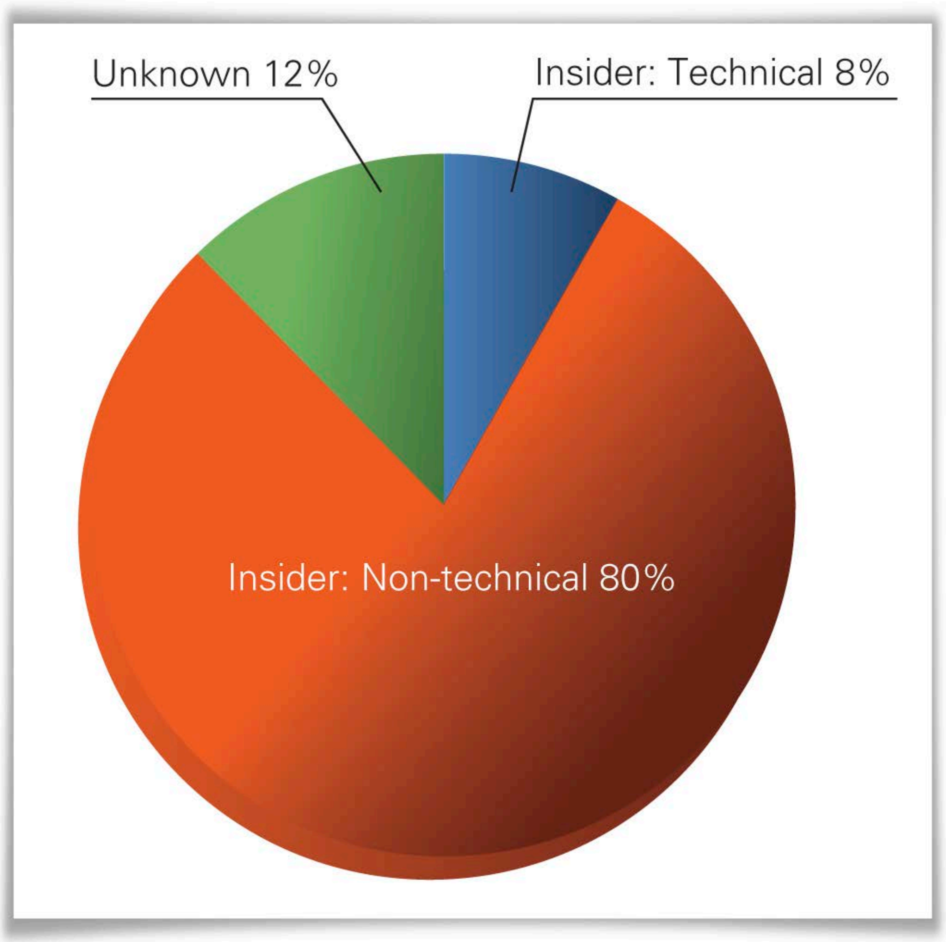
Crime: Created a fake employee on the payroll of one of the companies and in 6 years paid herself over $100,000.00

How Caught: The company owner discovered a large amount of cash missing from an account.

Consequences: Pled guilty to charges of wire fraud and check fraud; sentenced to 15 months in prison and 3 years' probation and was ordered to repay the remaining $77,000 of the stolen money

Finding Two: Low-Tech

Insiders’ means were not very technically sophisticated.



Non-technical subjects were responsible for 65 (81 percent) incidents.

Seven were external attackers, but their methods were also non-technical.

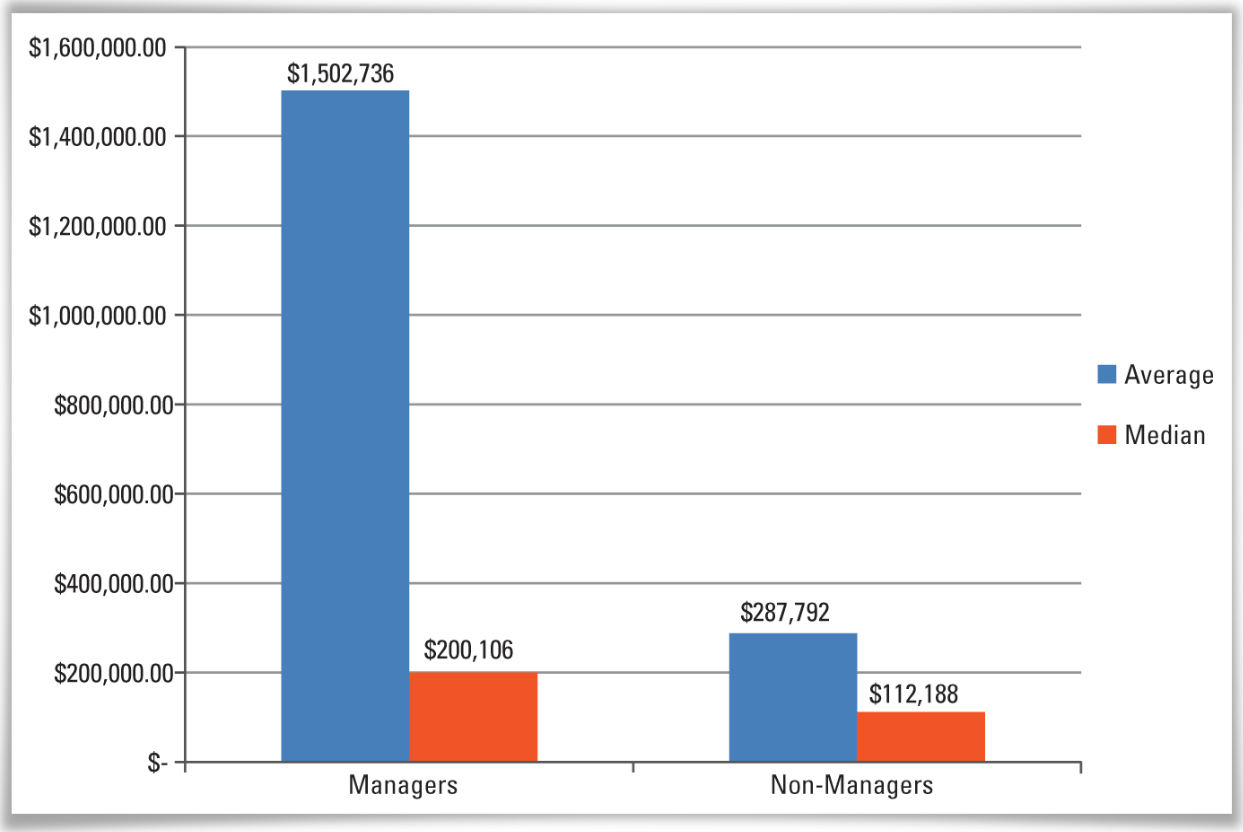
Finding Two: A Case Example

Non-Technical Subject: A vice president at a credit union given a corporate credit card to use only for business purposes

Crime: Used his corporate credit card for personal expenses and cash advances; created fake invoices on his business laptop; and created a fake contract with his wife’s third-party organization to pay it for fake services via wire transfer

Finding Three: Managers vs. Non-Managers

Fraud by managers differs substantially from fraud by non-managers by damage and duration.



Of 61 subjects, 31 (51 percent) were managers, VPs, bank officers, or supervisors. The median results show that managers consistently caused more actual damage ($200,106) than non-managers ($112,188).

Finding 3: Fraud Dynamic

While analyzing insider fraud cases, we discovered two dominant scenarios:

- Manager Scenario (32 cases)
- Non-Manager Employee Scenario (30 cases)

In the **Manager Scenario**, the perpetrators of fraud are typically branch managers or vice presidents who realize they are able to alter business processes, including influencing subordinate employees, in a way that suits their desire to profit financially.

In the **Non-Manager Employee Scenario**, the perpetrators are often customer service representatives who alter accounts or steal customer account or other PII to defraud the victim organization for money.

These scenarios share many patterns, but they each have some key distinguishing characteristics.

Finding 3: Comparison of Fraud by Managers and Non-Managers

Attribute	*Manager Fraud*	*Non-Manager Fraud*
Number of Cases	31	30
Position Held	branch manager, vice president	help desk employee, accountant, bank teller
Median Age	38	31
Timeline	extended duration	comparatively short
Origin of Trust	period of loyal service	inherent in duties and position
Possible Source of Others' Suspicions	subordinate social engineering	co-worker proximity to fraud acts
Outsider Facilitation	nearly nonexistent	financial source from perpetrated identity crime
Concealment	flying below the radar	unsophisticated deceptions

Finding Three: Managers vs. Non-Managers

	Categories of Non-Managers			
	Accounting	**Customer Service**	**Technical**	**Analyst**
Duration Average, (Months)	41	10	26	20
Average Damages, Actual	$ 472,096	$ 191,338	$ 104,430	$ 54,785
Damage per Month, Average	$ 11,627	$ 18,350	$ 4,041	$ 2,785

Non-Managers

On average, accounting employees did the most actual damage, followed by customer service employees and, with much less damage, technical and analysis employees.

Finding Three: A Case Examples

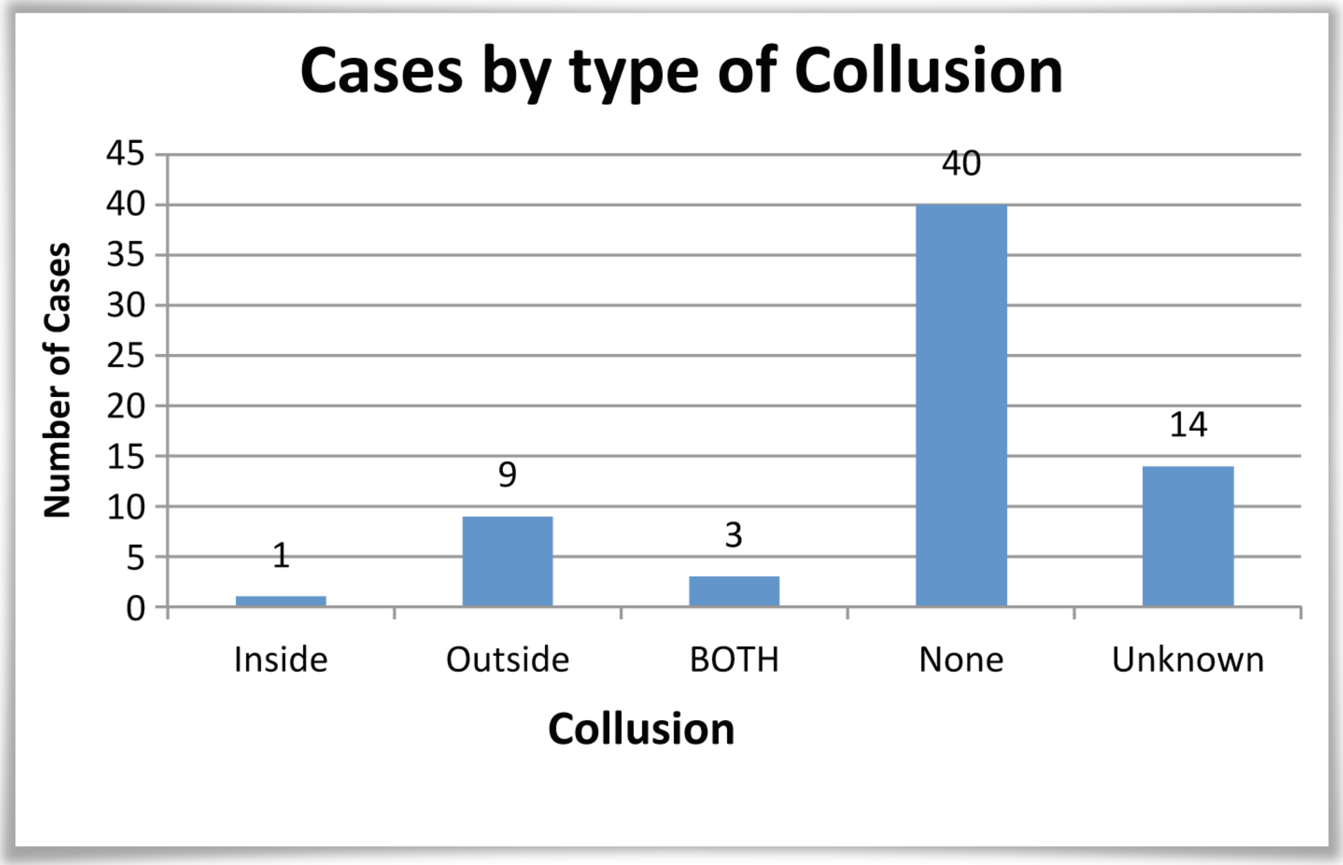
Technical Subject: A loan processor at a banking institution who had full privileges to read and modify loan information

Crime: Took out two legitimate loans totaling $39,000 for her own personal expenses, increased her personal loan amounts, and withdrew the difference thereby committing embezzlement

Damages: $112,000 was stolen

Finding Four: Collusion

Most cases do not involve collusion.



There was not a significant number of cases involving collusion, but those that did occur generally involved external collusion (i.e., a bank insider colluding with an external party to facilitate the crime).

Finding Five: Audits, Complaints, and Suspicions

Most incidents were detected through an audit, customer complaints, or co-worker suspicions.

The most common way attacks were detected was through routine or impromptu audits.

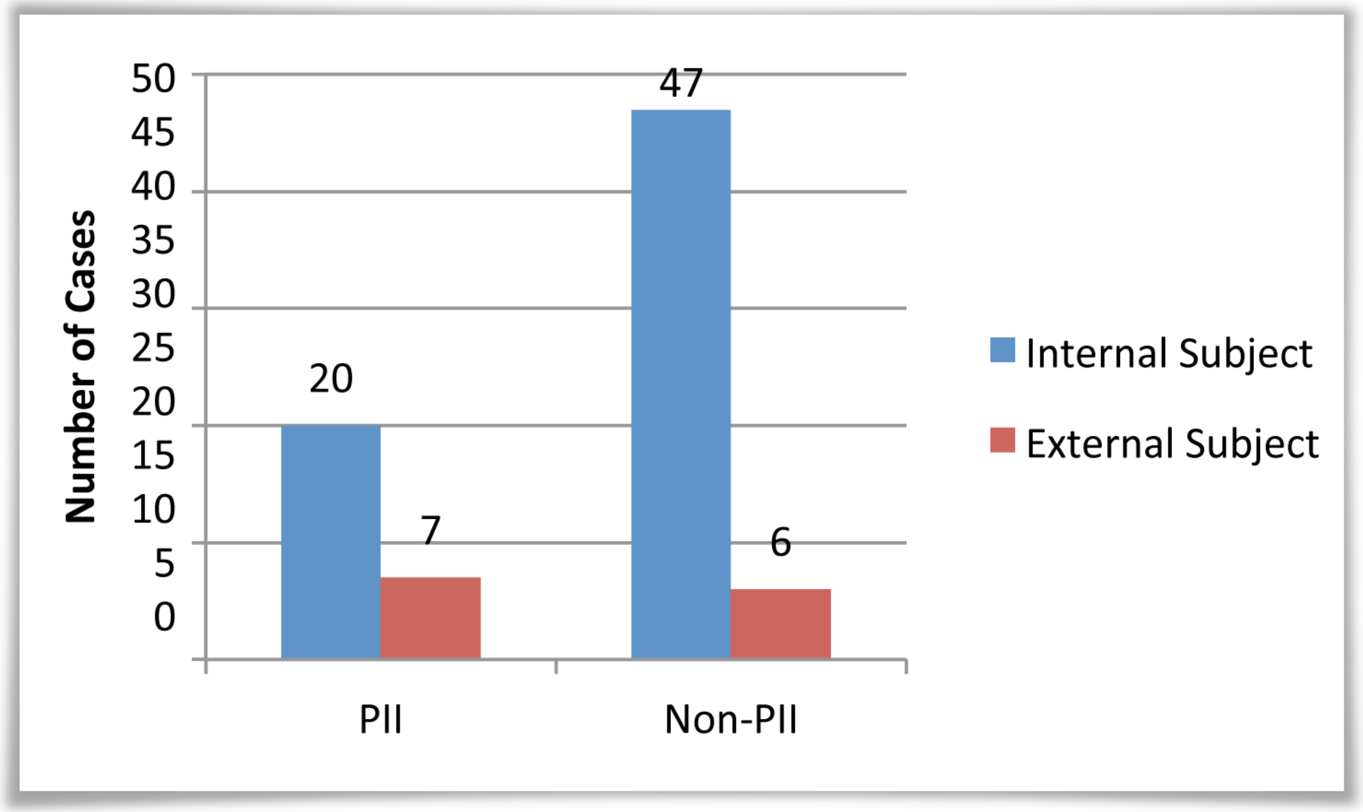
Over half of the insiders were detected by other victim organization employees, though none of the employees were members of the IT staff.

This fact, in conjunction with the mere 6 percent of cases where software and systems were used in detection, seems to indicate that fraud-detection technology was either ineffective or absent.

As expected, most initial responders to the incidents were managers or internal investigators (75 percent).

Finding Six: Personally Identifiable Information

Personally identifiable information (PII) is a prominent target of those committing fraud.



Of the 80 cases, 34 percent involved PII and 66 percent did not.
The external cases were evenly split between PII cases and non-PII cases.

Preventing Fraud After an Incident

Evaluate the fraud and ask the following questions:

- What business processes need to change?
- What new controls could be implemented to prevent similar activity in the future?
- What automated scripts are available that might detect similar activity?

Once you have the answers, take necessary steps, such as creating and running fraud-detection scripts, to help identify similar or ongoing fraud activity.

What You Can Do

Get copies of these documents

- *Insider Fraud in Financial Services*
- *Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector*
- *CERT Common Sense Guide to the Prevention and Detection of Insider Threats*

Reports available here:

www.cert.org\insider_threat\ - Insider Threat Center

www.sei.cmu.edu\financial_fraud_report\

www.sei.cmu.edu\financial_fraud_summary\

Consider the following seven strategies…

Policies and Controls

Clearly document and consistently enforce policies and controls.

- Enforce policy **consistently** to prevent employees from feeling they are being treated unfairly.
- Prevent the opportunity to commit fraud by consistently enforcing policies and **inconsistently** monitoring and auditing transactions.

Security Awareness Training

Institute periodic security awareness training for all employees.

- Ensure that each employee understands the security **policies** and the **process** for reporting policy violations.
- Ensure that all employees know that security policies and procedures exist, that there is a good reason why they exist, that they must be enforced, and that there can be serious **consequences** for infractions.
- Warn employees that individuals may try to **co-opt** them into activities counter to the organization's mission, including committing fraud.

Employee Reinvestigations

Include unexplained financial gain in any periodic reinvestigations of employees.

- Institute a periodic **reinvestigation** process for employees in positions of trust.
- Determine whether employees are under **significant financial stress**.
- Determine **unexplained wealth** or living beyond ones means.

Online Activity

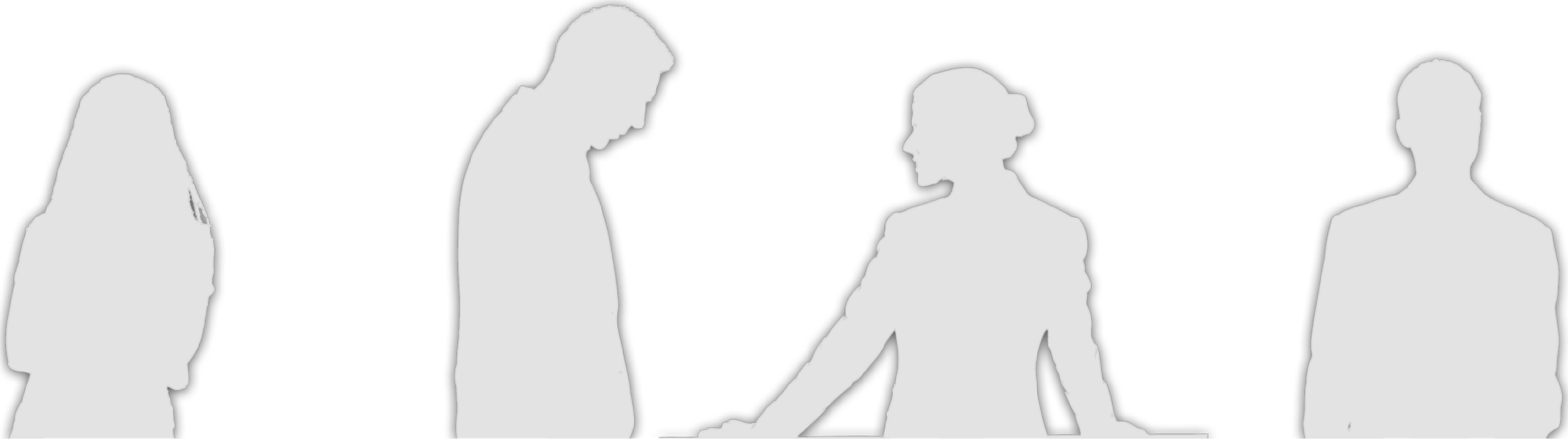
Log, monitor, and audit employee online actions.

- Enforce **account and password** policies and procedures to ensure that online actions can be associated with the employee who performed them.
- Use **logging**, periodic **monitoring**, and **auditing** to discover and investigate suspicious insider actions before more serious consequences occur.
- Use **SIEM** and **data-leakage tools** to detect unauthorized changes to the system and the downloading of confidential or sensitive information.

Accountants and Managers

Pay special attention to accountants and managers.

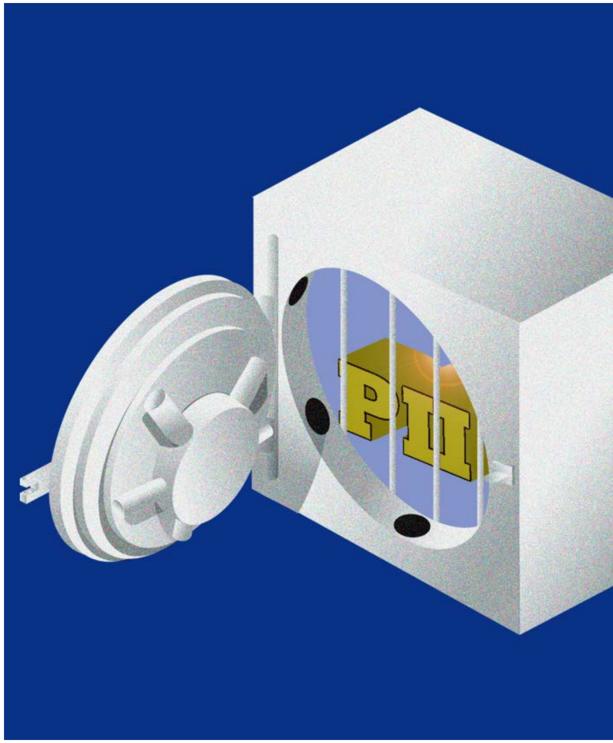
- Implement processes that “checks-the-checker.”
- Institute unpredictability into the auditing function.



Personally Identifiable Information

Restrict access to PII.

- Don’t allow privileges to **accumulate** over time.
- Ensure that employees have **appropriate privileges** to do their job duties, but not more than they need.
- Install controls to alert proper personnel when PII is **accessed**, **modified**, or **transmitted**.



Insider Incident Response Plan

Develop an insider incident response plan.

- Ensure that only those **responsible** for carrying out the plan understand and are trained on its execution.
- Use **lessons learned** to continually improve the plan.

Strategies for Insider Fraud Mitigation

- Clearly document and enforce policies and controls
- Institute periodic security awareness training for all employees
- Include unexplained financial gain in any periodic reinvestigations of employees
- Log, monitor, and audit employee online actions
- Pay special attention to accountants and managers
- Restrict access to PII
- Develop an insider incident response plan

Your Input and Feedback

We welcome ongoing information about **practices and technical solutions** that you have implemented to successfully counter insider threats.

Also, let us know if you want us to investigate anything not covered in this report that we can answer by querying and further analyzing our database of insider incidents.

Contact us at insider-threat-feedback@cert.org